



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/534,067	01/17/2006	Manxia Tie	C3110.0001	2699

32172 7590 07/21/2009
DICKSTEIN SHAPIRO LLP
1633 Broadway
NEW YORK, NY 10019

EXAMINER

AVERY, JEREMIAH L

ART UNIT	PAPER NUMBER
----------	--------------

2431

MAIL DATE	DELIVERY MODE
-----------	---------------

07/21/2009

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/534,067	Applicant(s) TIE ET AL.	
	Examiner JEREMIAH AVERY	Art Unit 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 May 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-21 is/are rejected.
- 7) ☒ Claim(s) 3 and 7 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 May 2005 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

I. Claims 1-21 have been examined.

Drawings

1. Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

2. Claims 3 and 7 are objected to because of the following informalities: punctuation error. There is a period in the middle of the claim language of claim 3, (i.e. "judge whether the certificate used by the other part is the same as the one informed by it. If it is not..."). Also, within claim 7, there is a period within the limitation labeled "5)", (i.e., "...secret key for conversation. If it is not..."). The period indicates that the claim has ended and thus any language after the period would not be part of the claim. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

Art Unit: 2431

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 21 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. The term "possibly" in claim 21 is a relative term which renders the claim indefinite. The term "possibly" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The term "possibly" renders the subsequent claim language indeterminate as to whether it is or is not fully utilized.

Claim Rejections - 35 USC § 102

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-16 and 19-21 are rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent No 7,350,076 to Young et al., hereinafter Young.

Art Unit: 2431

5. Regarding claim 1, Young teaches a method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link, wherein Mobile Terminal (MT) and Access Point (AP) perform the two-way certificate authentication through the Authentication Server (AS) (column 5, lines 42-66, column 10, lines 1-23 and column 12, lines 1-13 and 42-65); and MT and AP perform negotiation of secret key for conversation (column 10, lines 39-67, column 11, lines 1-9 and column 12, lines 32-41).

6. Regarding claim 2, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:
when MT logs on AP, MT and AP performs said two-way certificate authentication through AS (column 5, lines 42-66, column 10, lines 1-23 and column 12, lines 1-13 and 42-65);
after said two-way certificate authentication is successfully performed, MT and AP perform said negotiation of the secret key for conversation (column 10, lines 39-67, column 11, lines 1-9 and column 12, lines 32-41).

7. Regarding claim 3, Young teaches said method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:
when MT logs on AP, MT and AP inform one another of their respective certificate, and then they perform negotiation of secret key for conversation (column 10, lines 39-67, column 11, lines 1-9 and column 12, lines 32-41);

Art Unit: 2431

after said negotiation of secret key for conversation is completed, MT and AT performs the two-way certificate authentication through AS (column 5, lines 42-66, column 10, lines 1-23 and column 12, lines 1-13 and 42-65),

and meanwhile judge whether the certificate used by the other part is the same as the one informed by it. If it is not, the authentication fails; if it is, the result of the authentication depends on the result of said two-way certificate identification (column 10, lines 62-67, column 11, lines 1 and 2, "If the values do not match, then there is no authentication of the network device and the session is terminated. If the values match, then the network device 210 has shown that is a valid device for client device 202 and therefore the network device 210 is authenticated to the client device 202" and column 13, lines 21-37).

8. Regarding claim 4, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:
said two-way certificate authentication comprising the steps: 1) when MT logs on AP, MT sends to AP the access authentication request message containing the MT certificate; 2) after AP receives said access authentication request message, it adds the AP certificate to the message, then sends to AS the certificate authentication request message containing said MT certificate and AP certificate; 3) after AS receives said certificate authentication request message, AS authenticates the AP certificate and MT certificate in said message, and then sends back to AP the certificate authentication response message containing the AS signature; 4) after AP receives said certificate

Art Unit: 2431

authentication response message, AP authenticates the AS signature, so as to obtain the result of authentication of the MT certificate, and then sends back to MT the certificate authentication response message as the access authentication response message; and 5) after MT receives said access authentication response message, MT authenticates the AS signature and obtains the result of authentication of the AP certificate, so as to complete said two-way certificate identification between MT and AP (column 5, lines 42-66, column 10, lines 1-23 and column 12, lines 1-13 and 42-65).

9. Regarding claim 5, Young teaches said method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

1) when MT logs on AP, MT sends to AP the access authentication request message containing the MT certificate for said two-way certificate authentication; 2) after AP receives said access authentication request message, it adds the AP certificate to the message, then sends to AS the certificate authentication request message containing said MT certificate and AP certificate for said two-way certificate authentication, and meanwhile begins with MT negotiation of the secret key for conversation; 3) after AS receives said certificate authentication request message, AS authenticates the AP certificate and MT certificate in said message, and then sends back to AP the certificate authentication response message containing AS signature for said two-way certificate authentication; 4) after AP receives said certificate authentication response message, AP authenticates the AS signature, so as to obtain the result of authentication of the MT certificate, and then sends back to MT the certificate authentication response message

Art Unit: 2431

as the access authentication response message for said two-way certificate authentication; and 5) after MT receives said access authentication response message, MT authenticates the AS signature and obtains the result of authentication of the AP certificate, so as to complete the process of said two-way certificate identification between MT and AP (column 5, lines 42-66, column 10, lines 1-23 and column 12, lines 1-13 and 42-65), and then MT performs the corresponding processing to complete said negotiation of secret key for conversation (column 10, lines 39-67, column 11, lines 1-9 and column 12, lines 32-41).

10. Regarding claim 6, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

1) when MT logs on AP, MT sends AP the access authentication request message containing the MT certificate for said two-way certificate authentication; 2) after AP receives said access authentication request message, it adds the AP certificate to the message, then sends to AS the certificate authentication request message containing said MT certificate and AP certificate for said two-way certificate authentication; 3) after AS receives said certificate authentication request message, AS authenticates the AP certificate and MT certificate in said message, and then sends back to AP the certificate authentication response message containing AS signature for said two-way certificate authentication (column 5, lines 42-66, column 10, lines 1-23 and column 12, lines 1-13 and 42-65);

Art Unit: 2431

4) after AP receives said certificate authentication response message, AP authenticates the AS signature, so as to obtain the result of authentication of the MT certificate, AP judges the result of authentication. If the authentication is not successful, AP sends back to MT said certificate authentication response message as the access authentication response message for said two-way certificate authentication; If the authentication is successful, AP begins to consult with MT the secret key for to conversation while it sends back to MT said access authentication response message (column 10, lines 62-67, column 11, lines 1 and 2, "If the values do not match, then there is no authentication of the network device and the session is terminated. If the values match, then the network device 210 has shown that is a valid device for client device 202 and therefore the network device 210 is authenticated to the client device 202" and column 13, lines 21-37);

and 5) after MT receives said certificate authentication response message, MT authenticates the AS signature and obtains the result of authentication of the AP certificate, so as to complete said two-way certificate identification between MT and AP, and then MT performs the corresponding processing to complete said process of negotiation of secret key for conversation (column 10, lines 39-67, column 11, lines 1-9 and column 12, lines 32-41).

11. Regarding claim 7, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

Art Unit: 2431

1) when MT logs on AP, each part informs the other of its own certificate, then they complete said negotiation of secret key for conversation, and, meanwhile, MT also completes informing AP of the access authentication request identification; 2) AP sends to AS the certificate authentication request message containing the MT certificate and AP certificate for said two-way certificate Authentication; 3) after AS receives said certificate authentication request message, AS authenticates the AP certificate and MT certificate in said message, and then sends back to AP the certificate authentication response message containing AS signature for said two-way certificate authentication; 4) after AP receives said certificate authentication response message, AP authenticates the AS signature, so as to obtain the result of authentication of the MT certificate, and then sends back to MT said certificate authentication response message as the access authentication response message for said two-way certificate authentication (column 5, lines 42-66, column 10, lines 1-23 and column 12, lines 1-13 and 42-65); and 5) after MT receives said access authentication response message, MT authenticates the AS signature, and then judges whether the AP certificate is the same as the one AP informed of before negotiation of secret key for conversation. If it is not, the authentication fails; if it is, MT obtains the result of the authentication of the AP certificate from the message, so as to complete said two-way certificate authentication process between MT and AP (column 10, lines 62-67, column 11, lines 1 and 2, "If the values do not match, then there is no authentication of the network device and the session is terminated. If the values match, then the network device 210 has shown that

Art Unit: 2431

is a valid device for client device 202 and therefore the network device 210 is authenticated to the client device 202” and column 13, lines 21-37).

12. Regarding claim 8, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1 wherein: said access authentication request message also comprising the access authentication request identification (column 10, lines 62-67 and column 11, lines 1, 2, 10-27 and 40-50).

13. Regarding claim 9, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claims 4, 5, 6 or 7, wherein: said certificate authentication request message also comprising the access authentication request identification, or also comprising the access authentication request identification and AP signature (column 2, lines 44-56, column 10, lines 62-67 and column 11, lines 1, 2, 10-27 and 40-50).

14. Regarding claim 10, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein: said certificate authentication response message also comprising, before the signature filed of AS, the information of the result of the MT certificate authentication and those of the AP certificate authentication (column 10, lines 62-67 and column 11, lines 1, 2, 10-27 and 40-50).

Art Unit: 2431

15. Regarding claim 11, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

said access authentication response message is identical with said certificate authentication response message (column 2, lines 44-56, column 10, lines 62-67 and column 11, lines 1, 2, 10-27 and 40-50).

16. Regarding claim 12, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 7, 8 or 9 wherein:

said access authentication request identification is a string of random data *or* authentication serial number (column 10, lines 34-42 and 54-61, column 11, lines 10-17 and column 12, lines 20-31).

17. Regarding claim 13, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

said information of MT certificate authentication result comprising the MT certificate, and the MT certificate authentication result and the AS signature, or comprises the MT certificate and the MT certificate authentication result (column 10, lines 62-67 and column 11, lines 1, 2, 10-27 and 40-50).

18. Regarding claim 14, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

Art Unit: 2431

said information of the AP certificate authentication result comprises the AP certificate, the AP certificate authentication result, the access authentication request identification and the AS signature, *or* comprises the AP certificate, the AP certificate authentication result and the access authentication request identification (column 2, lines 44-56, column 10, lines 62-67 and column 11, lines 1, 2, 10-27 and 40-50).

19. Regarding claim 15, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

when MT intends to access to the designated AP, the MT must first of all obtain the relevant information of the AP or the certificate of the AP (column 2, lines 44-56, column 10, lines 62-67 and column 11, lines 1, 2, 10-27 and 40-50).

20. Regarding claim 16, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein: said negotiation of secret key for conversation refers to MT or AP using AP's or MT's common key and their respective own private key to generate the secret key for conversation (column 2, lines 46-56, "During the Diffie-Hellman key agreement exchange, both the wireless device and the access point sign the information used to generate the shared secret key and this information is forwarded to a trusted third party", column 10, lines 39-67, column 11, lines 1-9 and column 12, lines 32-41).

Art Unit: 2431

21. Regarding claim 19, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data

communication via wireless link according to claim 1, wherein:

said negotiation of secret key for conversation comprising: 1) MT or AP generates a string of random data, and sends them to AP or MT as the secret key negotiation request message after encryption using the common key of AP or MT; 2) After it receives said secret key negotiation request message from MT or AP, AP or MT uses its own private key for decryption, obtains the random data generated by the other part; then AP or MP generates again a string of random data; and sends them to MT or AP as the secret key negotiation response message after encryption using the common key of MT or AP; and 3) After it receives said secret key negotiation response message from AP or MT, MT or AP, uses its own private key for decryption, obtains the random data generated by the other part; both MT and AP utilizes the random data generated by the other part and itself to generate the secret key for conversation (column 2, lines 46-56, "During the Diffie-Hellman key agreement exchange, both the wireless device and the access point sign the information used to generate the shared secret key and this information is forwarded to a trusted third party", column 5, lines 56-66, column 10, lines 39-67, column 11, lines 1-17 and 33-39 and column 12, lines 14-19, 32-41 and 47-61).

22. Regarding claim 20, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data

communication via wireless link according to claim 1, wherein:

Art Unit: 2431

said negotiation of secret key for conversation comprising: 1) MT or AP generates a string of random data, and, after it utilizes the common key of AP or MT for encryption, attaches its own signature as the secret key negotiation request message, and transmits it to AP or MT; and 2) after AP or MT receives said secret key negotiation request message from MT or AP, it utilizes the common key of MT or AP to authenticate the signature, and then utilizes its own private key to decrypt the encrypted message received; both MT and AP uses the random data as the secret key for conversation (column 2, lines 46-56, "During the Diffie-Hellman key agreement exchange, both the wireless device and the access point sign the information used to generate the shared secret key and this information is forwarded to a trusted third party", column 5, lines 56-66, column 10, lines 39-67, column 11, lines 1-17 and 33-39 and column 12, lines 14-19, 32-41 and 47-61).

23. Regarding claim 21, Young teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:
said negotiation of secret key for conversation *possibly* also comprising negotiation of the communication algorithm used in the process of communication (column 10, lines 39-67, column 11, lines 1-9 and column 12, lines 32-41).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 2431

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Young as applied to claim 1 above, and further in view of United States Patent No. 5,515,439 to Bantz et al., hereinafter Bantz.

24. Young significantly teaches the claimed invention, as cited above. However, Young does not substantially teach the claim limitations found within claims 17 and 18. Bantz teaches said claim limitations, as cited below.

25. The motivation to combine would be "to provide such a method for dynamically transmitting and validating the value of any variable between two users of a communications network" (*Bantz* - column 2, lines 34-38).

26. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Bantz with the teachings of Young in order "to protect this exchange certificate against replay attacks" (*Bantz* – column 10, lines 21-30).

Art Unit: 2431

27. Regarding claim 17, Bantz teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data

communication via wireless link according to claim 1, wherein:

said negotiation of secret key for conversation comprising: 1) MT secretly chooses an integer a , from which to calculate the integer $f(a)$, combines the integer $f(a)$ and the MT signature on it into the secret key negotiation request message, and transmits it to AP; said f is a function rendering integer a from the integer $f(a)$ in calculable; 2) after it receives said secret key negotiation request message, AP secretly chooses an integer b , from which to calculate the integer $f(b)$, combines the integer $f(b)$ and the AP signature on it into the secret key negotiation response message, and transmits it to MT; said f is a function rendering integer b from the integer $f(b)$ in calculable; and 3) AP calculates $g(b, f(a))$, and MT calculates $g(a, f(b))$ after it receives said secret key negotiation response message, as the secret key for conversation in the process of communication; said g is a function rendering the calculation of $g(a, f(b))=g(b, f(a))$ possible (column 2, lines 57-67, column 3, lines 1-13 and 35-67, "cannot be solved for K' without knowledge of S ", column 4, lines 1-6, column 8, lines 36-61, column 9, lines 60-67 and column 10, lines 1-20, "an eavesdropper intercepting this exchange certificate cannot get knowledge of the value K' since he does not know the secret key S ").

28. Regarding claim 18, Bantz teaches the method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data

communication via wireless link according to claim 1, wherein:

Art Unit: 2431

said negotiation of secret key for conversation comprising: 1) AP secretly chooses an integer b , from which to calculate integer $f(b)$, combines the integer $f(b)$ and the AP signature on it into the secret key negotiation request message, and transmits it to MT; said f is a function rendering integer a from the integer $f(b)$ in calculable; 2) after it receives said secret key negotiation request message, MT secretly chooses an integer a , from which to calculate the integer $f(a)$, forms the integer $f(a)$ and the MT signature on it into the secret key negotiation response message, and transmits it to AP; said f is a function rendering integer a from the integer $f(a)$ in calculable; and 3) MT calculates $g(a, f(a))$, and AP calculates $g(a, f(b))$ after it receives said secret key response message, as the secret key for conversation in the process of communication; said g is a function rendering the calculation of $g(a, f(b))=g(b, f(a))$ possible (column 2, lines 57-67, column 3, lines 1-13 and 35-67, "cannot be solved for K' without knowledge of S ", column 4, lines 1-6, column 8, lines 36-61, column 9, lines 60-67 and column 10, lines 1-20, "an eavesdropper intercepting this exchange certificate cannot get knowledge of the value K' since he does not know the secret key S ").

Conclusion

29. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

30. The following United States Patents are cited to further show the state of the art with respect to secure network communication, such as:

United States Patent No. 6,912,657 to Gehrmann, which is cited to show a method and arrangement in a communication network.

Art Unit: 2431

United States Patent No. 7,246,236 to Stirbu, which is cited to show a method and apparatus for providing peer authentication for a transport layer session.

United States Patent No. 7,389,412 to Sharma et al., which is cited to show a scheme for device and user authentication with key distribution in a wireless network.

United States Patent No. 7,028,186 to Stenman et al., which is cited to show key management methods for wireless LANs.

United States Patent No. 7,107,620 to Haverinen et al., which is cited to show authentication in a packet data network.

31. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

32. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2431

33. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431